Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation

Ahmed Altaher, Stéphane Mocanu, Jean-Marc Thiriet

Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation

A. Altaher, S. Mocanu & J.-M Thiriet
Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France

ABSTRACT: Power substations are intensively renovated toward using information and communication technologies such as object oriented modeling and Ethernet networks. In the last two decades, Substation automation systems used capabilities of network communication services adopted from sophisticated international standardizations such as IEC 61850. Distributed safety related functions take advantage of these technologies to protect the process-level equipment. Substation devices such as intelligent electronic devices, measurement units and circuit breaker controllers, with new capabilities, i.e. enabling IEC 61850, are integrated to build the protection and control functions that form the safety-related system. The objective of this research is to evaluate quantitatively the dependability for transformer protection architectures in the bay level. Safety integrity levels model, described in both IEC 62061 and IEC 61508, gives measurements for safety integrity levels according to the probability of failure. The determination of these levels is an approach to estimate system dependability.

1 INTRODUCTION

Power grid reliability requirements enacted by international and national level standards require avoiding electrical service outages. The outage of power delivery must be in the range of no more than 5 minutes per year to achieve higher availability (99.999%).

In (Altaher et al. 2015), experimental setup was conducted to evaluate critical communication in a testbed of process-level network. The evaluation is done, with framework of the IEC 61850 standard, by implementing communication protocols.

In this paper we aim to investigate dependability of bay-level hardware architectures inside an IEC 61850-based distribution substation. Our approach uses reliability block diagrams and the safety integrity approach framework from the international standards IEC 61508, to investigate reliability, availability and safety availability in this context.

This paper is organized in five sections. Second section identifies briefly the electrical power grid. Third section introduces the IEC 61850 substation communication standard, its features and concepts; in sub-section 3 we emphasis a distribution substation. In section 4, we detail the dependability concept and its attributes. Proposed architecture with reliability and availability calculations are mentioned in sub-section 3 whereas sub-section 4 proposes an evaluation of the functional safety. Section 5 concludes the paper.

2 THE ELECTRICAL POWER GRID

The electrical power delivery follows many stages from power generation through transmission and distribution to the ultimate main load centers. Practically the electrical power grid composes of power stations, cabling system, transmission and distribution substations and related control centers. The interconnection of these subsystems becomes progressively intelligent forming the smart grid. The grid exchanges automatically real time, electrical power, parameters enabling utilities to manage and control remotely all components and to manipulate the grid reliability and safety (McDonald et al. 2013). Modern grids have telecommunication networks supporting distributed protection and control functions inside the substations. Further, the power system includes extra-high voltage (EHV) networks used to transmit electricity from power generation stations to distribution networks known as high-voltage (HV) networks. End consumers are connected to the distribution facilities, i.e. substations. Electrical substations build coordinated transmission and distribution nodes, which are configured by control centers

to maintain the health of the power grid. Smart technologies and intelligent devices protect and control substation functionalities either locally or remotely by means of information and communication technologies. The IEC 61850 standard, communication networks and systems in substations, drives interoperability between several substation devices, e.g. intelligent electronic devices (IEDs), from different vendors. Additionally, the standard provides flexible assignment of different functions that enhance safety-related functions (Brand et al 2004).

3 THE IEC 61850 STANDARD

The technical committee 57 (TC57), which belongs to The International Electro-technical Commission (IEC), has released the IEC 61850 standard to enforce interoperability and to enable abstraction of communication services (IEC TC57. 2010). Its parts manage standardization of different services dedicated for vertical and horizontal communications inside substation levels. It enables delivery of high-speed peer-to-peer messages for status and events exchange. The standards includes at least 10 parts, the first five parts identify general and specific functional requirements. Part 6 covers an engineering tools such as substation configuration language to manage the design configurations by allowing description of relations between substation functions, substation primary or/and secondary equipment. Part 7 includes 4 sub parts identifying abstraction and mapping of data services to communication protocols. Part 8 defines manufacturing message services (MMS) mapping to data services. Part 9 also has sub parts, part 9-1 defines mapping of sampled values (SV) and 9-2 deals with the Process-bus. Part 10 emphasizes procedures of conformance testing.

3.1 *IEC 61850 Standard features*

The substation automation systems benefit from the standard parts at different levels (station, bay and process levels). Inherited engineering models are enforced by the standard providing new capabilities such as object-oriented data modeling, communication mapping services, configuration tools such as substation configuration language, and new process-level instrumentation technologies. These capabilities paved the way for horizontal communications between distributed devices inside substation levels. In result, the IEDs cooperate in real-time, to enable distribution of functionalities, by using Ethernet network technology. The substation primary equipment is controlled by dedicated formal device function numbers (IEEE std. C37.2 2008). The IEC 61850 part 5 introduces standardized logical nodes (LN) to define these functions. Logical nodes are embedded into the IEDs to form logical devices that are defined by specific requirements. Obviously, the IEDs are programmable devices that provide protection and control functions. These devices contain logic solvers, input and output ports, network interfaces to gather information about the primary equipment via communication protocols. GOOSE (general object oriented substation events) messages are multi-casted from publishers (IEDs) to subscribers (IEDs) in real-time pattern. These messages are important for delivering status (data set) about primary equipment parameters, e.g. circuit breaker switch position and status. Other specific messages called sampled values (SV) are used to inform bay-level devices about the process-level measured physical parameters, i.e. voltage and current. Innovative merging units (MU) are used to convert analog parameters and to transmit synchronously the sampled values with precise time-synchronization (IEC 61850 part 9-2).

3.2 *The IEC 61850 object modeling*

The standard defines object models to enforce interoperability between IEDs from different vendors. These models help reducing costs and time required for configuration of SAS implementations, and improving engineering documentation. As mentioned earlier logical nodes are models that form basic functionalities. A logical node is the smallest part of a function that exchange data (IEC TC 57. 2010). It contains data object and methods used to create functional components of different classes. These classes provide different protection, measurement, control, monitoring functions in SAS operations. Among these IEC 61850 defined classes are XCBR circuit breaker, XSWI isolator or earth switch, TCTR Current transformer, YLTC power transformer, PTOC time overcurrent protection and ATCC automatic tap changer controller. Interoperability between logical nodes achieved through standardized data objects included in every logical node. Three levels of data modeling and services are considered. The first level is the abstract communication service interface (ACSI) that allocates models and associated services for accessing data and object elements. The second level is common data classes (CDC) that specify data attributes while the third level defines logical node classes and data classes. These levels represent hierarchical levels (Fig.1).

Alongside this concept, an intelligent electronic device, i.e. physical device PHD, could be constructed by one or several logical devices.

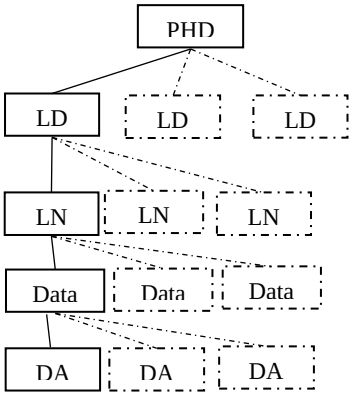

Figure 1. Hierarchical object modeling

3.3 *The distribution substation under study*

We choose the transformer bay (Fig. 2), in distribution substation, as a case study to analyze the functional components according to the IEC 61850 standard. We start by identifying specific components such as primary and secondary equipment. The primary equipment is the main process-level circuits composed of a bus bar, power lines, feeders and transformers, while secondary devices are bay-level auxiliary devices such as monitoring, protection and control devices. The bay-level in the substation is used logically between station-level and process-level equipment. The station-level consists of engineering computers, human machine interfaces, supervisory control and data acquisition, tele-control access, whereas the process-level is composed of electrical power equipment, e.g. circuit breakers.

Planning a SAS design requires drawing of a single line diagram (Fig. 2) that shows process-level components. Electromechanical equipment such as disconnectors and CBs are shown. The power transformer, i.e. converting high voltage into a lower voltage levels, converts 34.5 kV into 13.8 kV. This transformer bay forms a small distribution (D1-2) substation architecture (IEC 61850-1 2010). In other hand, additional components: bus bar, line, breakers and disconnectors are interconnected to construct the primary switchgear. These components are controlled by local/remote commands via a local Ethernet network. The bay-level would include protection and control IEDs that handle functionalities of the process-level and gather information about the equipment. The protection and control IEDs are interconnected via communication network (Fig. 2).

4 DEPENDABILITY OF SAS SYSTEMS

Dependability is defined as the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its users; a user is another system (human or physical) which interacts with the former (Laprie 1992). Additionally, it is defined as the ability to perform as and when required (IEC 60050-191). Dependability is a collective set of time-related performance characteristics that coexist with other requirements such as output, efficiency, quality, safety, security and integrity (Hardeveld & Kiang 2012).

4.1 *Reliability and availability of process level*

Reliability is defined as continuity of service, in other definition it is defined as a measure of continuous delivery of correct service or, equivalently, of time to failure (Laprie 1992) while IEC TC56 committee defines reliability as the probability that an item fulfils the required functions for the required duration.

In power utility communication systems, IEC 61850 part 3 section 4 considers reliability as quality requirement by focusing on communications for substation automation networking services. The standard provides a reference for other standards such as IEC 60870-4 that specifies performance requirements for tele-control. Further, IEC 61850 identifies the reliability of communications, inside the substation different levels, as data exchange without failure, loss or delay of critical messages. Precisely, there should be no single point of failure (SPOF) in substation networks. If failures exist, outcomes may cause damage to substation equipment.
The standard insists that communication reliability is needed as a requirement for substation automation; therefore, it recommends fail-safe design that should be handled to avoid undesired control action.

The availability is defined as readiness of usage, and as a measure of the delivery of correct service with respect to the alteration of correct and incorrect service (Laprie, 1992). IEC TC56 illustrates: “the availability is extent to which an item is operational and able to perform any required function or set of functions if a demand is placed on it”. Evidently, one can recognize the relation between the dependability attributes.

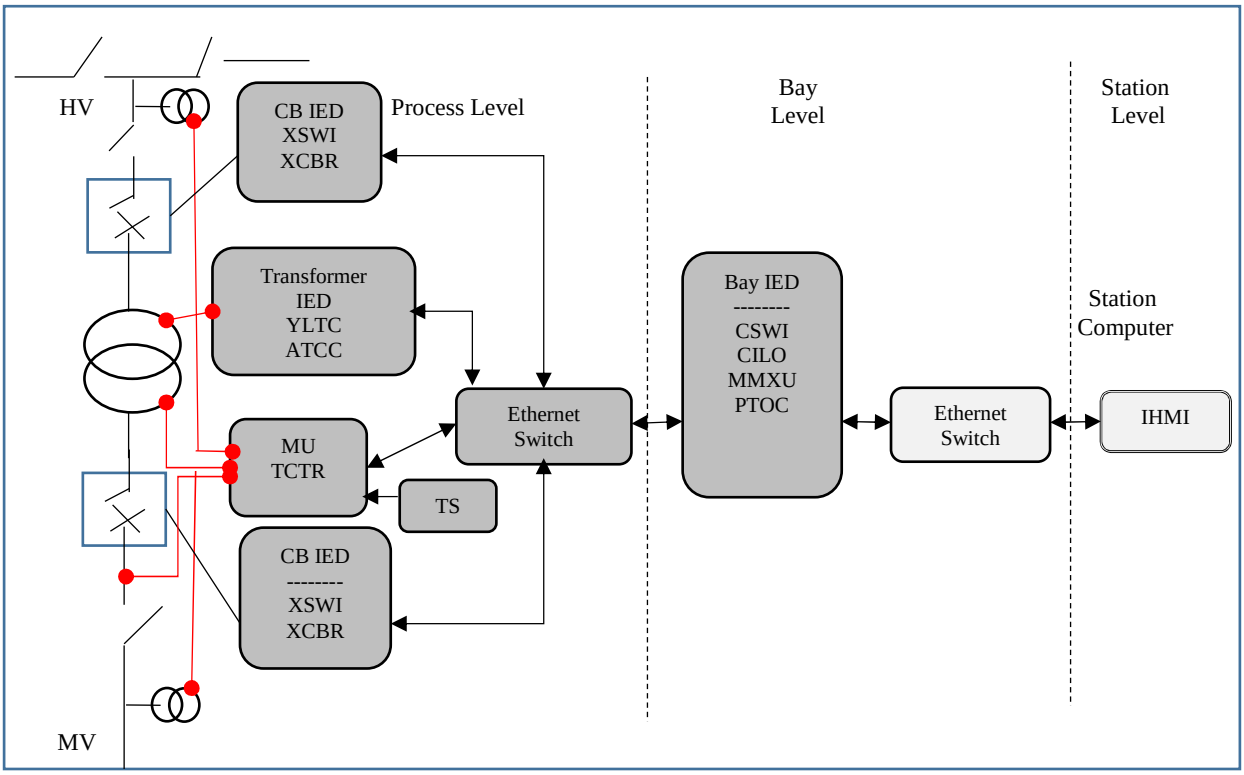

Figure.2 Substation communications among different levels, Logical Nodes within IEDs

The availability is derived from reliability, safety and integrity (Hardeveld & Kiang 2012). Hence, the dependability has different attributes (Laprie 1992) such as reliability, availability, safety and security. In addition, IEC TC56, which is responsible for dependability management standards, defines core dependability attributes that include reliability, availability, maintainability and maintenance support.

The current practice in the field of power transmission and distribution requires dependable networks to deliver continuous electrical energy. Power substations contribute directly to the power system reliability and availability. Transmission and distribution substations process-level equipment is the main concern for evaluating substation role on general power system reliability. The substation availability depends mainly on primary and secondary equipment failure rates, communication topology, redundancy, maintenance procedures and support…

In previous work (Altaher et al. 2015), the authors investigate reliability of process-level network within an IEC 61850 enabled communication services. In this paper, we aim to evaluate hardware architectures considering redundant components.

4.2 *Safety and functional safety*

Safety is avoidance of catastrophic consequences on people, property and environment; hence, reducing risk frequency and consequence is primary objective for safety systems. In this manner, safety is a measure of continuous safeness, or equivalently, of time to catastrophic failure (Laprie 1992).

Functional safety is a part of overall safety that depends on the correct functioning of the process or equipment in response to its inputs (IEC TC 65. 2010).

Protection functions in substations were found to be safety related with varying levels of risk (Purewal & Waldron 2004). These functions construct principal protection layer to prevent hazardous. Among these hazardous events are; short-circuits, arc flash and inter-phase short-circuits. Switchgear equipment faults could lead to critical failures such that failing to force sequential clearance of faults. In result, these events cause hazard consequences against substation technicians.

For practical design reasons, disconnectors in process-level are not able to switch on/off higher current loads (Zurakowski 2000). Technically, these disconnectors are used for isolation clearance between disconnected elements, which cannot be achieved by circuit breakers. Switching-off a line requires sequential procedure performed in timely adjusted mechanism to avoid any damage. Perfect example is when tripping circuit breaker, in case of failing or delayed command that might cause late reaction. Consequence could be an electrical arc accompanied by high rate optic and acoustic phenomena, causing spray of melted iron and flashovers.

Another consequences may include inter-phase short-circuit leading to damage of equipment and injury of nearby people.
The loss of disconnector would cost procurement of new equipment, replacement time, partial power outage and probability of critical accidents. E.g. the wrong switching-off of a loaded line by the related disconnector. The potential consequences will cost damage of process-level equipment and switchgear devices. In addition, substation disturbance could cause partial interruption of power distribution.
In (Prata et al. 2011) failure mode analysis was performed on MV substation to identify the components that were more likely to cause an interruption. That analysis has shown the most critical component in the studied substation is power transformer. Another failure mode analysis was done by (Zurakowski 2000) to evaluate risks and their consequences on HV power substations. In our study, we consider both; a) the above mentioned failure modes that cause risks for substation staff and switchgear equipment, and b) the risk matrix which is elaborated by (Prata et al. 2011).

4.3 *Integration and separation*

Many standards recommend separation of control systems from safety functions, e.g. Institute of Electrical and Electronics Engineering standards (IEEE) recommend that the safety system design shall be such other systems failures shall not prevent the safety system form meeting its requirements. Furthermore, ANSI/ISA (American National Standards Institute/International Society of Automation) mentioned that separation between basic process control system (BPCS) and safety instrumentation system (SIS) functions reduce the probability that both control and safety functions become unavailable at the same time, or that inadvertent changes affect the safety functionality of the SIS. Contrary, in many substation design requirements, protection and control systems are integrated. Functional safety imposes separation of protection functions from control system to avoid common cause failures.
In the protection and control, the process of specifying the degree of targeted safety should concern the associated risk assessment. Concerning the safety probability per function, designers of SAS safety-related functions estimate a tolerable failure with probability of 10^{-5}/h to 10^{-6}/h (Brand et al, 2004).
One measure for the functional safety is the probability of failure on demand when a system fails to respond to a demand for action arising from a potentially hazardous condition (IEC TC 65. 2010). This parameter increases during mission time or test interval.

4.4 *Reliability, availability and safety metrics*

For dependability evaluation, the combinatory model of reliability block diagram (RBD) is used to illustrate the functional components, and for analyzing different system architectures such as parallel, series, non-parallel and series. A system works if there is path of functioning components. Comparing other methods such as fault trees (FT), reliability graphs, Bayesian networks and Markov models, this model is an effective tool that provide flexibility to determine reliability of system by considering its components. Evaluation of dependability concerns; hardware components, communication network as component and redundancy of critical components to avoid single point of failure. Protection and control subsystems are allocated in series arrangements, while redundant components are represented by parallel arrangements. These arrangements are required when one subsystem replace another subsystem.
Assuming useful life period and constant failure rates (i.e. exponentially distributed lifetime), the following formulas give expressions for calculating reliability by given metrics such as mean time to failure (MTTF), mean time to repair (MTTR), i.e. average time from detecting the failure of a component until its replacement. Eq.1 gives an expression of failure rate as reciprocal of MTTF

$$\lambda_i = \frac{1}{MTTF_i} \tag{1}$$

Where, λ_i is failure rate of i^{th} component. The reliability function of component i is given by Eq.2:

$$R_i(t) = e^{-\lambda_i t} \tag{2}$$

Where t is the mission time for a component in useful life period.

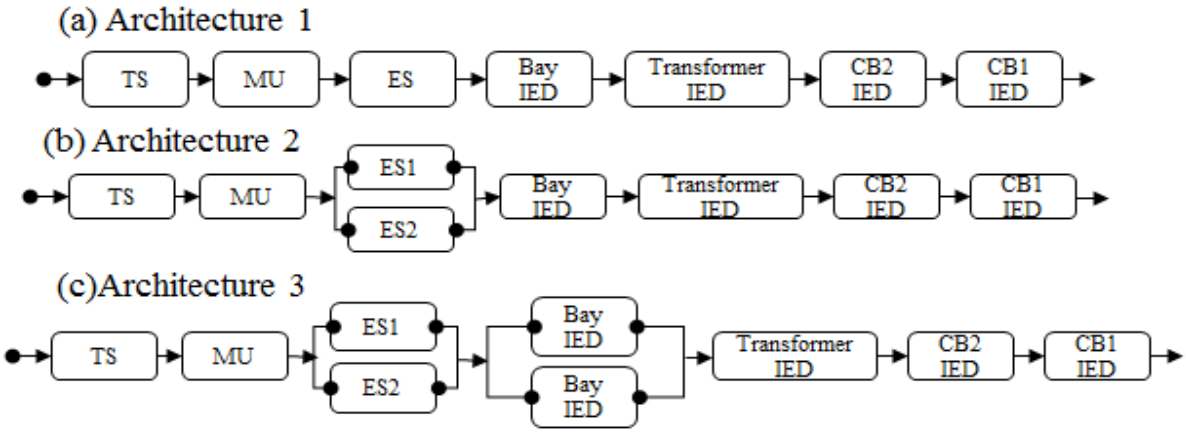

Figure.3: three different process/bay level architectures

Series system reliability, $R_s(t)$ is given by Eq.3, assuming independent failure of individual components.

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = e^{-(\sum_{i=1}^{n} \lambda_i)t} \quad (3)$$

Parallel system reliability (non-repairable components), $R_p(t)$, correspondingly, is given by Eq.4:

$$R_p(t) = 1 - \prod_{i=1}^{n} Q_i(t) \quad (4)$$

Where $Q_i(t)$ is the unreliability of i^{th} component, and it is given by Eq.5:

$$Q_i(t) = 1 - e^{-\lambda_i t} \quad (5)$$

Furthermore, to evaluate availability, following formulas use repair (μ) and failure (λ) rates to calculate the availability. Repair rate (replacing a component) is given by Eq.6:

$$\mu_i = \frac{1}{MTTR_i} \quad (6)$$

Then, availability A_i of i^{th} component will be calculated by using MTTF and MTTR metrics as given in Eq.7:

$$A_i = \frac{MTTF_i}{MTTF_i + MTTR_i} \quad (7)$$

Similarly, the availability formula, using repair and failure rates, is given in Eq.8:

$$A_i = \frac{\mu_i}{\mu_i + \lambda_i} \quad (8)$$

To evaluate the safety availability, tolerable risk/failure, non-protected failure is required to determine the risk reduction factor RRF. Eq.9 gives an expression to find the RRF:

$$RRF = \frac{F_{np}}{F_t} \quad (9)$$

Where F_{np} is the unprotected risk frequency that equals dangerous undetected failures, i.e. PFD for low demand and PFH for high demand, and Ft is tolerable risk frequency which is mentioned early (see section 4.3). PFDavg is given by Eq.10:

$$PFD_{avg} = \frac{1}{RRF} \quad (10)$$

where RRF represents the risk reduction factor. In Eq.11, safety availability is given by knowing the PFDavg.

$$SA = 1 - PFD_{avg} \quad (11)$$

The following table (Table 1) contains the MTTF values that are obtained from (Brand et al 2003, Lindquist et al 2008), these figures will be used for reliability, availability and safety availability calculations.

Table 1: Components MTTF and MTTR values

Component	MTTF (Years)	MTTR (Hours)
Bay IED	150	8
Ethernet Switch	50	4
Merging Unit	150	8
CB IED	100	8
Transformer IED	150	8
Time source	150	4

From the given metrics, reliability, i.e. mission time is 1000 hours, and availability are calculated for the three architectures (table 3).

Table 2: Safety Integrity Levels and the Probability of Failures on Demand

Safety Integrity Levels	1	2	3	4
Safety Availability	90%-99%	99%-99.9%	99.9%-99.99%	Non relevant
Risk Reduction Factor	10 to 100	100 to 1000	1000 to 10,000	10,000 to 100,000
Average Probability of Failure on Demand-Low rate demand	$>=10^{-2}$ to 10^{-1}	$>=10^{-3}$ to 10^{-2}	$>=10^{-4}$ to 10^{-3}	$>=10^{-5}$ to 10^{-4}
Failure rate (λ) per hour - high rate demand	$>=10^{-6}$ to 10^{-5}	$>=10^{-7}$ to 10^{-6}	$>=10^{-8}$ to 10^{-7}	$>=10^{-9}$ to 10^{-8}

The results are given in table 3 as following:

Table 3: Protection and control architectures reliability and availability

Architecture	Reliability %	Availability %
Basic	99.24185353	99.99512951
Redundant Ethernet	99.31740880	99.99604270
Redundant Bay IED	99.34260667	99.99665150

Transformer protection and control function is a SRS function that simultaneously controls line, bus bar and transformer bays equipment, including controlling transformer tap position, CB and disconnectors switches tripping (opening). This function does operate in continuous (high mode). Considering (table 2), high demand rate requires probability of failure rates per hour (PFH) which is the average dangerous frequency of failure per hour of components or subsystems.

The IEC 61508 standard sets SIL level according to dangerous failure rates as explained in table 3. We assume as in the standard (IEC TC 65. 2010) that statistically only every other failure is a potentially dangerous failure. For complex devices failure modes are assumed and divided as 50% safe and 50% dangerous. This assumption is explained in Eq.12.

$$\lambda_D = \lambda_s = \frac{1}{2} \times \lambda \tag{12}$$

The Eq.1 thus holds for $\lambda_{D,}$ which equals in this case $1/MTTF_{D,}$ for determining both dangerous undetected λ_{DU} failure rate and dangerous detected $\lambda_{DD,}$ Eq.13 and Eq.14 are used:

$$\lambda_{DU} = \lambda_D \times (1 - DC) \tag{13}$$

$$\lambda_{DD} = \lambda_D \times DC \tag{14}$$

The channel equivalent mean down time (t_{CE}) is calculated according to the standard in Eq.15

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \times (\frac{T1}{2} + MTTR) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \tag{15}$$

In this manner we can determine the probability of failure per hour PFH in Eq.16

$$PFH = 1 - e^{-\lambda dt_{ce}} \tag{16}$$

For redundant components with MooN structure, designers should consider common cause failures, represented by β factor (IEC TC 65. 2010). For 1oo2 structure, we assume that β=0.04, and β_D=0.02,i.e. dangerous common cause factor, for both redundant Ethernet switches and bay IEDs. PFH is given by:

$$PFH = 2 \times ((1 - \beta_D) \times \lambda_{DD} + (1 - \beta) \times \lambda_{DU})^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times (\frac{T1}{2} + MTTR) \tag{17}$$

Where t_{GE} (group down time) is given by Eq.18:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \times (\frac{T1}{3} + MTTR) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \tag{18}$$

and DC is the (automatic) diagnostic coverage (assumed 90% coverage) and T1 is the proof-test interval (assumed 1 month). Eq.19 gives the total failure rate of the SIF system (series):

$$\lambda_{ser} = \sum_{i=1}^{n} \lambda_i \tag{19}$$

For two identical components with constant failures, the total failure rate, i.e. 1oo2 redundancy is given by Eq.20

$$\lambda_{par} = \frac{2\lambda_i}{3} \tag{20}$$

4.5 *Calculating functional safety metrics*

The above-mentioned formulas are used for estimating the PFH of the three safety related architectures (Fig. 3) and the results are tabulated in (table 4).

Table 4: probability of failure per hour (PFH) and safety availability of SRS functions for proposed architectures

Architecture	PFH	Safety Availability %
Basic	3.8E-06	99.9996
Redundant Ethernet	2.7E-06	99.9997
Redundant Bay IED	2.3E-06	99.9998

From table 3 and table 4, we can notice clearly that two architectures with redundant components are satisfying IEC 61850 requirement, i.e. avoiding single point of failure, the architecture 3 has a higher reliability protection function regarding its lower dangerous failure and overall failure rate. These architectures are all suitable for SIL 1 level (high demand). Figure 4 illustrates decreasing of the reliability with mission time increasing.

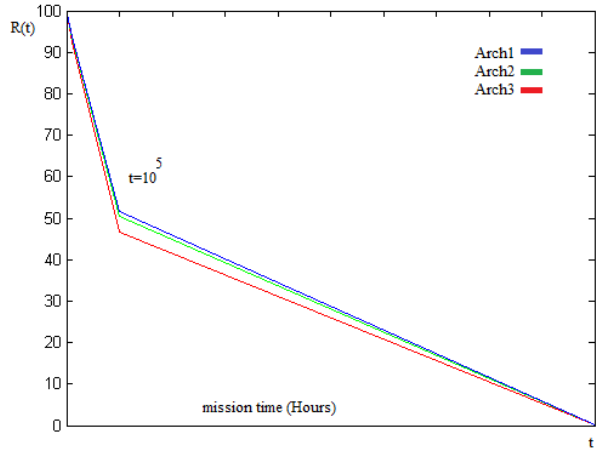

Figure.4: reliability of the three architectures

5 CONCLUSION AND FUTURE WORK

We evaluate three process-level architectures by applying classical reliability methods. Safety availability of these architectures is evaluated by using functional safety approach.

First architecture is basic well-known process-level/bay-level topology, which already exists in many distribution substations. The second proposed architecture benefits from Ethernet switch redundancy to eliminate SPOF in case of communication faults, furthermore, the third proposed architecture uses redundant bay device to increase availability of main-bay protection and control. In future research, we will evaluate availability of shared logical nodes, therefore a detailed analysis of Ethernet communication network traffic, and the switching mechanism in relation with worst-case load will be performed

6 REFERENCES

Altaher A., Mocanu S., Thiriet J.-M. (2015). Evaluation of Time-Critical communications for IEC 61850- Substation Network Architecture, Surveillance 8, *Proc. Intern. Conf.* 20-21 October, Roanne, France.

Brand, K. P., Lohmann, V., & Wimmer, W. (2003). Substation automation handbook. Bremgarten: Utility Automation Consulting Lohmann.

Brand, K.P., Brunner C., Wimmer W. (2004). Design of Based Substation Automation Systems According to Customer Requirements, *In CIGRÉ 2004 (Conseil International des Grands Réseaux Électriques).* Paris: CIGRÉ.

Hardeveld Van, T. & Kiang, D, 2012. Practical Application of Dependability Engineering. *American Society of Mechanical Engineers*. New York: ASME Press

IEC, TC57 (2010). IEC 61850: Communication networks and systems for power utility automation. *International Electro technical Commission Std*. Geneva: IEC.

IEEE std. C37.2 (2008). Electrical Power System Device Function Numbers and Contact Designation. *Intern. Std.* New York: IEEE.

IEC 60050-191:1990/AMD2:2002. (2002). International Electro-technical Vocabulary - Chapter 191: Dependability and quality of service, International Electro technical Commission Std. Geneva: IEC.

IEC, TC 65 (2010). IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems, International Electro technical Commission Std. Geneva: IEC, 2010.

Laprie, J. C. 1992. Dependability: basic concepts and terminology in English, French, German, Italian and Japanese, in A. *Avizienis*, H. Kopetz, J.C Laprie (eds.), *Dependable computing and fault tolerance systems* 5:3-43, Vienna: Springer.

Lindquist, T. M., Bertling, L., & Eriksson, R. 2008. Circuit breaker failure data and reliability modelling. Generation, Transmission & Distribution, IET, 2(6), 813-820, Nov. 2008.

McDonald, J. D., Wojszczyk, B., Flynn, B., & Voloh, I. (2013). Distribution Systems, Substations, and Integration of Distributed Generation. *In M. Begovic (ed). Electrical Transmission Systems and Smart Grids.* 1:7-68. New York: Springer.

Prata R., Ms Carvalho P., Afm Ferreira L. (2011). Failure Risk Associated with Different Substation and HV network Configurations. in 21st International Conference on Electricity Distribution. Proc. Intern. Conf., Frankfurt 6-9 June 2011:paper 0824.

Purewal S. & Waldron M.A. 2004. Functional safety in application of programmable devices in power system protection and automation. *Eighth IEE International Conference on Developments in Power System Protection; Proc. Intern. Conf. Amsterdam 5-8 April, 2004:*295-298.

Zurakowski Z. (2000). Safety and Security Issues in Electric Power Industry. *In F. Koornneef, & M. van der Meulen. (eds.), Computer Safety, Reliability, and Security: 19th International Conference, SAFECOMP 2000, Rotterdam, The Netherlands, October 24-27, Proc. Intern. Conf. Berlin: Springer.*